ELSEVIER

Theoretical Computer Science 266 (2001) 951–974

Theoretical Computer Science

www.elsevier.com/locate/tcs

Type inference for set theory

Raymond Turner *, [1]

Department of Computing Science, University of Essex, Wivenhoe Park, Colchester CO4 3SQ, UK

Received June 1999; revised December 2000; accepted January 2001
Communicated bu M. Nivat

Abstract

Weak set theories are employed for *set-theoretic specification*. We develop and explore *type inference systems* for such set theories. © 2001 Elsevier Science B.V. All rights reserved.

MSC: primary 05C38; 15A15; secondary 05A15; 15A18

Keywords: Set theory; Type inference; Specification

1. Type inference in specification

Specification languages based upon some form of set theory are now quite common. Z [4, 13, 15] and **VDM** [8, 6] are the most prominent examples but there are others. All these languages require only some very weak fragment of **ZF**. In particular, Z requires less than Zermelo set theory to formulate its set theoretical constructions and for **VDM** some version of admissable set theory will do.

In addition to the actual set theory, these systems come equipped with an associated *type inference system*. In the case of Z this is explicitly presented in [11, 12]. As a consequence specifications can be *type-checked* in much the same way that programs can. However, there has been very little theoretical investigation of such type systems. Their most elementary properties have not been explored; indeed, even their formulations are not entirely satisfactory. This is stark contrast to the highly developed type inference systems for programming languages [10] and theories of operations based upon the Lambda calculus [1].

The aim of this paper is to clarify some of the fundamental issues concerning such systems for set theory. We provide a basic type inference system for set theory and

* Corresponding author.
E-mail address: turnr@essex.ac.uk (R. Turner).
[1] URL: http://www.essex.ac.uk

PII: S0304-3975(01)00123-2

establish some of its elementary properties. We investigate a central question concerning the role of such systems in practice and explore the *completeness* of the type inference system with respect to its host set theory. Finally, we consider extensions to this basic theory which enable larger fragments of set theory to be the subject of type inference.

2. MacLane set theory

We employ a very weak theory of sets which is essentially **ZF** without replacement and with separation restricted to Δ_0-wff. It is known in the literature under two names: weak Zermelo [5] and MacLane set theory [7, 9]. It is certainly enough to formulate all the constructions of Z [3] and indeed for set-theoretic specification generally.

2.1. The language of **M**

In order to develop expressive type inference engines for set theory we need to postulate a richer syntax for the theory than the standard one. The syntax is given as follows where we employ lower case Greek letters for wff, x, y, z, etc., for variables and s, s_1, s_2, t, t_1, t_2, etc., for set terms generally:

$$s ::= x \mid \Phi \mid I \mid \{s, s\} \mid \cup s \mid Ps \mid \{x \in s \cdot \phi\},$$

$$\phi ::= s = s \mid s \in s \mid \Omega \mid \phi \to \phi \mid \phi \wedge \phi \mid \forall x \in s \cdot \phi.$$

Wff are formed from the atomic assertions of equality, membership and absurdity by implication, conjunction and bounded universal quantification. The set terms include variables together with terms for the empty set, an infinite set, pairs, unions, power sets and separation sets. We write $FV(e)$ for the set of free variables of any expression (term/wff) e. In quantification and separation $x \notin FV(s)$. Negation is defined as $\neg\phi \triangleq \phi \to \Omega$. We assume the standard classical definitions of the other connectives. Inclusion and extensional equivalence are also defined in the standard way: $x \subseteq y \triangleq \forall z \in x \cdot z \in y$ and $x \equiv y \triangleq x \subseteq y \wedge y \subseteq x$.

2.2. Rules and axioms of **M**

For uniformity and convenience, we employ a sequent style version of natural deduction for both the set theory and its type inference system. For the set theory, where Γ is a finite (possibly empty) set of wff, we write

$$\Gamma \vdash_{\mathbf{M}} \phi$$

(or just $\Gamma \vdash \phi$) just in case the sequent is derivable via the following rules. We shall, where no confusion can arise, leave out contexts and write axioms as rules with no premises.

2.2.1. ***Structural rules:***

$$\phi \vdash \phi \qquad \frac{\Gamma \vdash \psi}{\Gamma, \phi \vdash \psi}$$

2.2.2. ***Equality:*** In the second (the elimination/replacement) rule s and t must be *free for x in ϕ*:

$$s = s, \quad \frac{s = t \quad \phi[s/x]}{\phi[t/x]}$$

2.2.3. ***Logical rules:*** In the elimination rule for universal quantification t must be *free for x in ϕ*:

$$\frac{\Omega}{\phi} \quad \frac{\neg\phi \vdash \Omega}{\phi} \quad \frac{\phi \quad \psi}{\phi \wedge \psi} \quad \frac{\phi \wedge \psi}{\phi} \quad \frac{\phi \wedge \psi}{\psi}$$

$$\frac{\phi \vdash \psi}{\phi \to \psi} \quad \frac{\phi \to \psi \quad \phi}{\psi}$$

$$\frac{x \in s \vdash \phi}{\forall x \in s \cdot \phi} \quad \frac{\forall x \in s \cdot \phi \quad t \in S}{\phi[t/x]}$$

2.2.4. ***Extensionality:***

$$\frac{s \equiv t}{s = t}$$

2.2.5 ***Empty set:***

$$\forall x \in \Phi \cdot \Omega$$

2.2.6. ***Pairing:***

$$\frac{t = s_1 \vee t = s_2}{t \in \{s_1, s_2\}} \quad \frac{t \in \{s_1, s_2\}}{t = s_1 \vee t = s_2}$$

2.2.7. ***Union:***

$$\frac{\exists x \in s \cdot t \in x}{t \in \cup s} \quad \frac{t \in \cup s}{\exists x \in s \cdot t \in x}$$

2.2.8. ***Power set:***

$$\frac{t \subseteq s}{t \in Ps} \quad \frac{t \in Ps}{t \subseteq s}$$

2.2.9 ***Separation:*** For each wff $\phi[x]$, where *t is free for x in ϕ*

$$\frac{t \in s \wedge \phi[t/x]}{t \in \{x \in s \cdot \phi\}} \quad \frac{t \in \{x \in s \cdot \phi\}}{t \in s \wedge \phi[t/x]}$$

Since all wff are Δ_0, this only yields Δ_0-separation.

2.2.10 ***Infinity:*** The set I satisfies the *closure* axiom

$$0 \in I \wedge \forall y \in I \cdot succ(y) \in I,$$

where the numbers are introduced by definition as follows:

$$0 \triangleq \Phi,$$

$$succ(x) \triangleq \{x\}.$$

We shall also assume that I satisfies *induction* given as

$$\forall z \in PI \cdot (0 \in z \wedge \forall y \in I \cdot y \in z \rightarrow succ(y) \in z) \rightarrow z = I.$$

This is a conservative extension since such a set is already guaranteed by separation from a set satisfying the first axiom. However, it is more convenient to take such a set as basic.

Another slight modification which will facilitate the construction of the type system involves introducing the numbers as new primitives and replacing the above definitions by the following *axioms of representation*:

$$0 = \Phi,$$

$$\forall x \in I \cdot succ(x) = \{x\},$$

where the syntax for set terms now takes the extended form

$$s ::= x \mid \Phi \mid 0 \mid succ(s) \mid I \mid \{s,s\} \mid \cup s \mid Ps \mid \{x \in s \cdot \phi\}.$$

Such an addition is clearly a definitional one. However, it is necessary for formulating the type inference system.

This completes our presentation of the set theory **M**. It is much less parsimonious than the standard formulation of MacLane set theory which is usually stated without set terms; the axioms guarantee the existence of the sets. In this form the unbounded quantifiers are required. However, the addition of unbounded quantifiers is conservative over the present version of the theory since Maclane set theory only permits Δ_0 -separation: this guarantees that any model of the present theory can be extended to a model of standard Maclane.

3. A type inference system for M

Type inference systems are to be employed to reason about the *types* of **M**-expressions and, ultimately, to establish that *specifications* written in the language of **M** are *well-typed*. The following is the most basic type inference system for **M** and arises naturally from its finite ordinal structure.

3.1. The system T

The types of the system are just the finite ordinals. However, to avoid confusion with the natural numbers of the theory we use the following BNF definition.

$$\tau ::= i \mid P\tau$$

Judgements in the system are made relative to a type assignment *context* c which is a finite partial function from variables to types. Such a c will be represented as

$$x_1 : \tau_1, \ldots, x_m : \tau_m$$

where no variables is assigned more than one type. Since contexts are partial functions we adopt the following convenient notation. Let $c = x_1 : \tau_1, \ldots, x_m : \tau_m$ be a context. We write $dom(c)$ for $\{x_1, \ldots, x_m\}$ and $c(x_i)$ for τ_i. Where $v \subseteq dom(c)$, we write $c \restriction v$ for the restriction of c to v and $c \backslash x$ for $c \restriction \{y \in dom(c) \cdot y \neq x\}$. We write $c \subseteq c'$ to indicate that c' is an extension of c. We write $c, x : \tau$ for $c \cup \{x : \tau\}$ (provided that if $x \in dom(c)$ then $c(x) = \tau$) and $c; x := \tau$ for $c \backslash x, x := \tau$, the updated context. We shall say that a context c *covers* a term/wff e if $FV(e) \subseteq dom(c)$.

There are two judgements in **T**,

$$c \vdash s : \tau$$

$$c \vdash \phi \ prop$$

We write Θ for a judgement of either kind. The system is determined by the following rules.

3.1.1 ***Structural rules:***

$$c, x : \tau \vdash x : \tau \qquad \frac{c \vdash \Theta}{c, x : \tau \vdash \Theta}$$

3.1.2. ***Propositional formation rules:***

$$c \vdash \Omega \ prop$$

$$\frac{c \vdash s_1 : \tau \quad c \vdash s_2 : \tau}{c \vdash s_1 = s_2 \ prop} \qquad \frac{c \vdash s_1 : \tau \quad c \vdash s_2 : P\tau}{c \vdash s_1 \in s_2 \ prop}$$

$$\frac{c \vdash \phi \ prop \quad c \vdash \psi \ prop}{c \vdash \phi \wedge \psi \ prop} \qquad \frac{c \vdash \phi \ prop \quad c \vdash \psi \ prop}{c \vdash \phi \rightarrow \psi \ prop}$$

$$\frac{c, x : \tau \vdash \phi \ prop \quad c \vdash s : P\tau}{c \vdash \forall x \in s \cdot \phi \ prop} \quad x \notin FV(s)$$

3.1.3. ***The empty set, power set and separation:***

$$\Phi : Pi \qquad \frac{c \vdash s : P\tau}{c \vdash Ps : PP\tau}$$

$$\frac{c, x : \tau \vdash \phi \ prop \quad c \vdash s : P\tau}{c \vdash \{x \in s \cdot \phi\} : P\tau}$$

3.1.4. ***Union and pairing:***

$$\frac{c \vdash s : \tau \quad c \vdash t : \tau}{c \vdash \{s, t\} : P\tau} \qquad \frac{c \vdash s : PP\tau}{c \vdash \cup s : P\tau}$$

3.1.5. ***Natural numbers:***

$$0 : i \quad \frac{c \vdash s : i}{c \vdash succ(s) : i} \quad I : Pi$$

There are some immediate derived rules for the other logical connectives:

$$\frac{c \vdash \phi \ prop \quad c \vdash \psi \ prop}{c \vdash \phi \vee \psi \ prop} \qquad \frac{c \vdash \phi \ prop}{c \vdash \neg\phi \ prop}$$

$$\frac{c, x : \tau \vdash \phi \ prop \quad c \vdash s : P\tau}{c \vdash \exists x \in s \cdot \phi \ prop}$$

This completes the basic description of the system.

3.2. Basic properties of **T**

We consider some elementary properties of the system which parallel the results for the lambda calculus given in [1]

Lemma 1. (1) *If* $c \vdash \Theta$ *and* $c \subseteq c'$ *then* $c' \vdash \Theta$.
(2) *If* $c \vdash \Theta$ *then* c *covers* Θ.
(3) *If* $c \vdash \Theta$ *then* $c \restriction FV(\Theta) \vdash \Theta$.

Proof. By induction on the derivations. All are simple to verify. □

The next is the standard generation lemma which forms the basis of a type-checking algorithm: using it we can decide whether $c \vdash \Theta$ by driving the system *bottom up*.

Lemma 2 (Generation). (1) *If* $c \vdash s_1 \in s_2 \ prop$ *then for some* τ, $c \vdash s_1 : \tau$ *and* $c \vdash s_2 : P\tau$.
(2) *If* $c \vdash s_1 = s_2 \ prop$ *then for some* τ, $c \vdash s_1 : \tau$ *and* $c \vdash s_2 : \tau$.
(3) *If* $c \vdash \{x \in s \cdot \phi\} : \sigma$ *then* σ *has the form* $P\tau$ *and* $c; x : \tau \vdash \phi \ prop$ *and* $c \vdash s : P\tau$.
(4) *If* $c \vdash Ps : \sigma$ *then* σ *has the form* $PP\tau$ *and* $c \vdash s : P\tau$.
(5) *If* $c \vdash \phi \circ \psi \ prop$ *then* $c \vdash \phi \ prop$ *and* $c \vdash \psi \ prop$ $(\circ = \wedge, \rightarrow)$.
(6) *If* $c \vdash \forall x \in s \cdot \phi \ prop$ *then for some* $\tau, c; x : \tau \vdash \phi \ prop$ *and* $c \vdash s : P\tau$.
(7) *If* $c \vdash succ(t) : \sigma$ *then* σ *is* i *and* $c \vdash t : i$.
(8) *If* $c \vdash \cup s : \sigma$ *then* σ *has the form* $P\tau$ *and* $c \vdash s : PP\tau$.
(9) *If* $c \vdash \{s_1, s_2\} : \sigma$ *then* σ *has the form* $P\tau$ *and* $c \vdash s_i : \tau$.

Proof. All parts are routine by induction on the derivations. We illustrate with (6). $c \vdash \forall x \in s \cdot \phi \ prop$ can only be the conclusion of a derivation whose last rule applied is an instance of the structural rule of thinning or the rule for universal quantification itself. If the latter, the result is immediate. Suppose that it is the result of an application of thinning:

$$\frac{c \vdash \forall x \in s \cdot \phi \ prop}{c, y : \sigma \vdash \forall x \in s \cdot \phi \ prop}$$

We apply the induction hypothesis to the premise of the rule to yield

$$c; x : \tau \vdash \phi \ prop \quad c \vdash s : P\tau$$

We then apply thinning:

$$c, y : \sigma; x : \tau \vdash \phi \ prop \quad c, y : \sigma \vdash s : P\tau$$

Note that if $y = x$ the first rule follows immediately since the first assignment to y is discarded. □

Lemma 3 (Unicity). *If $c \vdash s : \tau$ and $c \vdash s : \sigma$ then τ and σ are the same type.*

Proof. By induction on the terms using the generation lemma. □

We also have the following admissable rules of substitution.

Lemma 4 (Substitution). (1) *If $c \vdash s : \tau$ and $c, x : \tau \vdash \phi$ prop then $c \vdash \phi[s/x]$ prop.*
(2) *If $c \vdash t : \tau$ and $c, x : \tau \vdash s : \sigma$ then $c \vdash s[t/x] : \sigma$.*
(3) *If $c \vdash \phi[s/x]$ prop then $c \vdash s : \tau$ and $c; x : \tau \vdash \phi$ prop for some τ.*
(4) *If $c \vdash s[t/x] : \sigma$ then $c \vdash t : \tau$ and $c; x : \tau \vdash s : \sigma$ for some τ.*

Proof. (1) and (2) are by induction on the wff/terms using the generation lemma. All the cases are easy to verify. The last two parts are also by induction on expressions. We illustrate with quantification. Suppose that

$$c \vdash \forall y \in s \cdot \phi[t/x] \ prop$$

Use the generation lemma, followed by the induction hypothesis followed by the type rule for quantification. □

More insight about the system can be gleaned from the idea of *raising* a type assignment context. Let c be a context. The raised context c^+ is obtained by raising the type of each variable by one, i.e. $x : \tau$ is in c iff $x : P\tau$ is in c^+. Similarly, where defined, the context c^- is obtained by reducing the type of each variable by 1.

Lemma 5 (Raising). *(i) If $c \vdash \phi$ prop then $c^+ \vdash \phi$ prop.*
(ii) If $c \vdash s : \tau$ then $c^+ \vdash s : P\tau$.

Proof. By induction on the derivations in **T**. □

Let c, c' be two contexts with $dom(c) \subseteq dom(c')$. We shall write

$$c \preccurlyeq c'$$

just in case for each $x \in dom(c)$, $c(x) \leqslant c'(x)$. We shall say that a context c which covers ϕ is *minimal* for ϕ if $c \vdash \phi$ prop and for all c' such that $c' \vdash \phi$ prop, $c \preccurlyeq c'$. Similarly for set terms.

Lemma 6. (1) *If* $c \vdash \phi$ *prop then there is a minimal context* c' *for* ϕ.
(2) *If* $c \vdash s : \tau$ *then there is a minimal context* c' *for* s.

Proof. For example, suppose $c \vdash \phi$ *prop*. If c^- is not defined then c is minimal. If it is defined and $c^- \nvdash \phi$ *prop* then c is minimal. Otherwise examine c^{--}. Obviously, this process must stop. □

3.3. Universes

We can now begin to explore the structure imposed upon **M** by this type system. Inside the set theory we define *universes* which are the set theoretic analogues of the types:

$$V_i \triangleq I,$$

$$V_{P\tau} \triangleq PV_\tau.$$

For any type context c, consider the context for **M** which contains $x \in V_\tau$ just in case $c(x) = \tau$. We shall also write c for this **M** context. We now indicate some elementary properties of these universes. The following can be established by a simple induction on the derivations in **T**.

Proposition 1. *If* $c \vdash_T s : \tau$ *then* $c \vdash_M s \in V_\tau$.

We also have a form of *foundation* for these universes.

Proposition 2. *For each type* τ

$$\forall x \in V_\tau \cdot x \notin x.$$

Proof. By induction on the types. For the base case we have only to note that, by numerical induction, $\forall x \in I \cdot x \in x \leftrightarrow x = succ(x)$. For the induction step suppose that $x \in V_{P\tau}$. Then suppose that $x \in x$. Then $\exists y \in x \cdot y = x$. By extensionality, $\forall z \in x \cdot z \in y$. Hence, $y \in x \wedge y = x \wedge y \in y$. But $x \in V_{P\tau}$ implies $y \in V_\tau$ and this contradicts the induction hypothesis. □

Finally, we observe that the universes are cumulative.

Proposition 3. *For each type* τ,

$$V_\tau \subseteq V_{P\tau}.$$

Proof. By induction on the types. For the base case we have only to note that, by numerical induction, $\forall x \in I \cdot x = \Phi \vee \exists y \in I \cdot x = \{y\}$. For the induction step suppose that $x \in V_{P\tau}$. Thus $x \subseteq V_\tau$. By induction, $\forall y \in x \cdot y \in V_{P\tau}$. Hence, $x = \{y \in V_{P\tau} \cdot y \in x\}$.

□

Proposition 4 (Inclusion). *For all types* τ_1, τ_2 *there exists a type* σ *such that type* $V_{\tau_1}, V_{\tau_2} \subseteq V_\sigma$.

4. Stratified theories

In set theoretic specification the language of set theory is employed as the host language for the construction of specifications; type inference systems are employed to *type-check* them. However, the set theory is also to be used to reason about the properties of specifications. This raises a question about the *legitimacy* of *proofs* in **M**: presumably, we would not want to obtain a property of a *legitimate* specification via a proof which contains *illegitimate* wff.

4.1. The theory $\mathbf{M}_T$

To be more precise about this we set up a formal system in which all wff are well-typed. We shall write

$$\Gamma \vdash^c \phi$$

if the sequent follows from the following rules. We adopt all the rules of **M** for the logic but guarded by type inference side conditions. In fact we only need to explicitly provide these conditions for the following rules:

$$\frac{c \vdash_{\mathbf{T}} \phi \ prop}{\phi \vdash^c \phi} \qquad \frac{\Gamma \vdash^c \psi \quad c \vdash_{\mathbf{T}} \phi \ prop}{\Gamma, \phi \vdash^c \psi}$$

$$\frac{\Gamma \vdash^c \Omega \quad c \vdash_{\mathbf{T}} \phi \ prop}{\Gamma \vdash^c \phi} \qquad \frac{c \vdash_{\mathbf{T}} s{:}\,\tau}{\vdash^c s = s}$$

The other rules remain as before but with the decoration, i.e.

$$\frac{\Gamma_1 \vdash \phi_1 \cdots \Gamma_n \vdash \phi_n}{\Gamma \vdash \phi} \quad \text{becomes} \quad \frac{\Gamma_1 \vdash^c \phi_1 \cdots \Gamma_n \vdash^c \phi_n}{\Gamma \vdash^c \phi}$$

For the sets we adopt all the rules/axioms for the empty set, separation and power set in their decorated form; the rules for union and pairing are now dropped. I is still taken to satisfy closure and induction in their decorated form but the axioms of representation are dropped since they are no longer stratified; these are replaced by the standard axioms for zero and successor.

The following is still true: use induction on the derivations in **T**:

$$If \ c \vdash_T s : \tau \ then \ c \vdash^c s \in V_\tau$$

The following is established by induction on the derivations in $\mathbf{M_T}$.

Theorem 1. *If* $\Gamma \vdash^c \phi$ *then* $\Gamma \vdash_{\mathbf{M}} \phi$.

Theorem 2. *If* $\Gamma \vdash^c \phi$ *then for each* $\gamma \in \Gamma \cup \{\phi\}$ *we have*

$$c \vdash \gamma \ \textit{prop}.$$

Proof. We use induction on the derivations in $\mathbf{M_T}$. For example consider $\forall$-introduction. By induction, the premises yield both that $c \vdash_{\mathbf{T}} x \in s$ *prop* and $c \vdash_{\mathbf{T}} \phi$ *prop*. By generation, $c \vdash_{\mathbf{T}} s : P\tau$ and $c \vdash_{\mathbf{T}} x : \tau$. Hence, $c \vdash_{\mathbf{T}} \forall x \in s \cdot \phi$ *prop*. □

4.2. The theory **KF**

A theory which is intermediate between **M** and $\mathbf{M_T}$ is the theory **KF** due to Kane and Forster [7]. To introduce it we require the following notion.

Definition 1. A wff ϕ is stratified iff $c \vdash \phi$ *prop* for some covering c. A set term s is stratified iff $c \vdash s : \tau$ for some covering c and type τ. A sequent $\Gamma \vdash \phi$ is stratified iff for some covering c, $c \vdash \gamma$ *prop* for each $\gamma \in \Gamma \cup \{\phi\}$.

Lemma 7 (Sub-formula). *If* e (*term or wff*) *is stratified and* e' *is a sub-term/sub-formula of* e *then* e' *is stratified*

Proof. Use the generation lemma. □

Definition 2. KF is the theory obtained from **M** by restricting the separation axiom schema to stratified wff.

Obviously, **KF** is an extension of $\mathbf{M_T}$ and can be interpreted in **M**. We shall explore the other directions as a corollary to the following.

5. Stratification

Our objective is to show that any stratified theorem of **M** is a theorem of $\mathbf{M_T}$. To this end we set up an interpretation of **M** into $\mathbf{M_T}$. The interpretation is given relative to a type assignment context c. Let e be any expression (term/wff), and c any context which c covers it. We define the translation of e relative to c, denoted by

$$|e|_c$$

by recursion on the structure of e.[1] As we proceed we shall establish, by induction on the structure, that $|e|_c$ is stratified by c.

[1] This construction is inspired by that of [5, 14, 9]. However, crucially, the current treatment of the natural numbers is different.

5.1. The interpretation

We begin the translation with the following clauses for wff:

$$|\Omega|_c \triangleq \Omega, \tag{1}$$

$$|\phi \to \psi|_c \triangleq |\phi|_c \to |\psi|_c, \tag{2}$$

$$|\phi \wedge \psi|_c \triangleq |\phi|_c \wedge |\psi|_c, \tag{3}$$

$$|\forall x \in s \cdot \phi|_c \triangleq \forall x \in |s|_c \cdot |\phi|_{c;x:=\tau} \quad \text{if } c \vdash |s|_c : P\tau. \tag{4}$$

In these cases the stratification of the *rhs* follows directly from the structural induction and the rules of **T**. We next deal with the easy cases of terms

$$|x|_c \triangleq x, \tag{5}$$

$$|0|_c \triangleq 0, \tag{6}$$

$$|\Phi|_c \triangleq \Phi, \tag{7}$$

$$|succ(s)|_c \triangleq \begin{cases} succ(|s|_c) & \text{if } c \vdash |s|_c : i, \\ 0 & \text{otherwise,} \end{cases} \tag{8}$$

$$|I|_c \triangleq I, \tag{9}$$

$$|Ps|_c \triangleq P|s|_c \quad \text{if } c \vdash |s|_c : P\tau, \tag{10}$$

$$|\cup s|_c \triangleq \cup|s|_c \quad \text{if } c \vdash |s|_c : PP\tau, \tag{11}$$

$$|\{x \in s \cdot \phi\}|_c \triangleq \{x \in |s|_c \cdot |\phi|_{c;x:=\tau}\} \quad \text{if } c \vdash |s|_c : P\tau. \tag{12}$$

Once again, by structural induction and the rules of **T**, each rhs is stratified relative to c.

This brings us to the easy cases of membership and equality. For equality we want to maintain extensionality; this demands the following has to be true:

(a) $|s_1 = s_2|_c \leftrightarrow |(\forall x \in s_1 \cdot x \in s_2)|_c \wedge |(\forall x \in s_2 \cdot x \in s_1)|_c$

For membership we require the following logical truth to be upheld.

(b) $|s_1 \in s_2|_c \leftrightarrow |\exists x \in s_2 \cdot x = s_1|_c$

Given our clauses for the bounded quantifiers this leads to the following clauses for equality and membership:

$$|s_1 = s_2|_c \triangleq (\forall x \in |s_1|_c \cdot |x \in s_2|_{c;x:=\tau}) \wedge (\forall x \in |s_2|_c \cdot |x \in s_1|_{c;x:=\sigma}), \tag{13}$$

where $c \vdash |s_1|_c : P\tau$ and $c \vdash |s_2|_c : P\sigma$,

$$|s_1 \in s_2|_c \triangleq \exists x \in |s_2|_c \cdot |x = s_1|_{c;x:=\sigma} \quad \text{where } c \vdash |s_2|_c : P\sigma. \tag{14}$$

To show that the rhs are stratified we require a sub-induction on the type *rank* of equality/membership statements where the *rank* of such an expression is defined as

$$rank(|s_1 \in s_2|_c) = rank(|s_1 = s_2|_c) = \tau_1 + \tau_2 \quad \text{where } c \vdash |s_i|_c : \tau_i.$$

As we proceed, we shall prove, by induction on the rank:

For all terms s_1, s_2 *and covering* c, *if* $|s_1|_c$ *and* $|s_2|_c$ *are*

stratified by c, *then so are* $|s_1 \in s_2|_c$ *and* $|s_1 = s_2|_c$.

Consider (13) and (14). First observe that by the main induction we may assume that $|s_1|_c$ and $|s_2|_c$ are stratified by c. Then observe that the rank of any $\|_c$ equality/membership expression occurring in the right hand side of (13)/(14) is less than any in the left. Using the rank induction hypothesis it is easy to see that in both cases the rhs are stratified.

This brings us to the cases where terms of type i are involved. The central question concerns the interpretation of membership in elements of type i. Given that we wish to maintain the standard representation of the natural numbers, the only member of a type i object will be its predecessor; 0 has no members. This leads to the following clauses for quantification where, by structural induction and the rules of **T**, the rhs is stratified:

$$|\forall x \in s \cdot \phi|_c \triangleq \forall x \in I \cdot succ(x) = |s|_c \to |\phi|_{c;x:=i} \quad \text{where } c \vdash |s|_c : i. \tag{15}$$

Next consider membership in objects of type i. Our general logical constraint on the interpretation membership (b), leads directly to the following clause:

$$|s_1 \in s_2|_c \triangleq \exists x \in I \cdot |s_2|_c = succ(x) \wedge |x = s_1|_{c,x:=i} \quad \text{where } c \vdash |s_2|_c : i. \tag{16}$$

For equality, the extensionality constraint (a) leads to

$$|s_1 = s_2|_c \triangleq |s_1|_c = |s_2|_c \quad \text{where } c \vdash |s_j|_c : i,\ j = 1,2, \tag{17}$$

$$|s_1 = s_2|_c \triangleq \forall x \in I \cdot |s_1|_c = succ(x) \to |x \in s_2|_{c;x:=i} \wedge \forall x \in |s_2|_c \cdot |x \in s_1|_{c;x:=i}, \tag{18}$$

where $c \vdash |s_1|_c : i$ and $c \vdash |s_2|_c : P\tau$.

Observe that, (13), (14), (16)–(18) taken together, ultimately yield that the rank of the terms on the right is less than those on the left. By the rank induction and the rules of **T**, the rhs are stratified. This concludes all the membership and equality cases – given that the component expressions are stratified, all the translations of these atomic wff are stratified.

Next we deal with the translation of terms involving type i objects. The above demands upon membership lead to the following clauses:

$$|Ps|_c \triangleq \{x \in I \cdot \forall y \in I \cdot succ(y) = x \to |y \in s|_{c;y:=i}\} \tag{19}$$

where $c \vdash_T |s|_c : i$,

$$|\cup s|_c \triangleq \begin{cases} \{x \in I \cdot succ(succ(x)) = |s|_c\} \\ \quad \text{where } c \vdash |s|_c : i, \\ \{x \in I \cdot \exists y \in |s|_c \cdot y = succ(x)\} \\ \quad \text{where } c \vdash |s|_c : Pi, \end{cases} \tag{20}$$

$$|\{x \in s \cdot \phi\}|_c \triangleq \{x \in I \cdot succ(x) = |s|_c \wedge |\phi|_{c;x:=i}\} \tag{21}$$

where $c \vdash |s|_c : i$.

Each of the rhs of (19) and (20) can easily seen to be stratified – the separation case (21) invokes the structural induction hypothesis.

Finally, we deal with pairing

$$|\{s_1, s_2\}|_c \triangleq \{x \in V_\sigma \cdot |x = s_1|_{c;x:=\sigma} \vee |x = s_2|_{c;x:=\sigma}\} \tag{22}$$

where $c \vdash_T |s_i|_c : \tau_i$ and $V_\sigma = V_{\tau_1} \cup V_{\tau_2}$.

Note that this makes sense by Proposition 4 and the fact that clause (b) for membership is maintained. By the main induction, the translation is stratified – given that equality is. This completes the definition of the translation. Summarizing, we have:

Theorem 3. *For each e and covering c,*

$|e|_c$ *is stratified by c.*

Thus each expression is translated to a stratified one.

5.2. Soundness

We now establish that the translation is sound, i.e. theorems of **M** translate to theorems of $\mathbf{M_T}$. Most of the work is contained in the following lemmata.

Lemma 8 (Equality). *For any covering c*:
(1) $\vdash^c |s = s|_c$,
(2) $\vdash^c |s_1 = s_2 \to s_2 = s_1|_c$,
(3) $\vdash^c |(s_1 = s_2 \wedge s_2 = s_3) \to s_1 = s_3|_c$,
(4) $\vdash^c |(s_1 = s_2 \wedge s \in s_1) \to s \in s_2|_c$,
(5) $\vdash^c |(s_1 = s_2 \wedge s_1 \in s) \to s_2 \in s|_c$.

Proof. All are routine. We argue by case analysis on the types of the expressions. We illustrate matters with (4) where $c \vdash |s_1|_c : i$ and $c \vdash |s_2|_c : P\tau$. Given the antecedent, the definitions yield

$$\forall x \in I \cdot |s_1|_c = succ(x) \to |x \in s_2|_{c;x:=i} \wedge$$

$$\exists x \in I \cdot |s_1|_c = succ(x) \wedge |x = s|_{c;x:=i}.$$

Hence, by (3), $\exists y \in |s_2|_c \cdot |y = s|_{c,y:=\tau}$. □

Lemma 9 (Replacement). *For terms s_1, s_2 and wff ϕ, covered by c:*
(1) $\vdash^c |s_1 = s_2 \to (\phi[s_1/x] \to \phi[s_2/x])|_c$,
(2) $\vdash^c |s_1 = s_2 \to (s[s_1/x] = s[s_2/x])|_c$.

Proof. By simultaneous induction on the terms/wff. All the cases are simple to verify except those for atomic wff and these are direct consequences of the previous lemma. □

Lemma 10 (Lifting). *For any c*

$$\vdash^c \forall x \in V_\tau \cdot \exists y \in V_{P\tau} \cdot |x = y|_{x:=\tau, y:=P\tau}.$$

Proof. By induction on the types. The only case that is not straightforward is the base case where we have to prove

$$\forall x \in I \cdot \exists y \in PI \cdot |x = y|_{x:=i, y:=Pi}.$$

We use numerical induction. If $x = 0$ then we put $y = \{x \in I \cdot x \neq x\}$. For $succ(x)$ it follows from the translation that

$$|succ(x) = \{z \in I \cdot z = x\}|_{x:=i}. \qquad \square$$

Lemma 11 (Extensionality). $\vdash^c |t \equiv s|_c \to |t = s|_c$.

Proof. We have to check each of the cases generated by the various combinations of types for the terms. However, each case is immediate given the definition of the translation which has been framed with extensionality as one of the main objectives. □

Lemma 12 (Power set). $\vdash^c |t \in Ps|_c \leftrightarrow |\forall x \in t \cdot x \in s|_c$.

Proof. The case where $c \vdash |s|_c : P\tau$ is straightforward to verify. The case where $c \vdash |s|_c : i$ requires some work. By the translation for membership and soundness of replacement we may assume $c \vdash |t|_c : i$. In this case, the lhs unpacks to

$$\exists x \in I \cdot \forall y \in I \cdot succ(y) = x \to x = |s|_c \wedge |t = x|_{c;x:=i}.$$

Given that $c \vdash |t|_c : i$, this is equivalent to the rhs. □

Lemma 13 (Union). $\vdash^c |t \in \cup s|_c \leftrightarrow |\exists x \in s \cdot t \in x|_c$.

Proof. The case where $c \vdash |s|_c : PP\tau$ is easy to verify. To illustrate the other cases consider the case where $c \vdash |s|_c : i$. By the translation for membership and soundness

of replacement we can concentrate on the case where $c \vdash |t|_c : i$. In this case, the lhs is equivalent to

$$succ(succ(|t|_c)) = |s|_c,$$

which is equivalent to the rhs. □

Lemma 14 (Pairing). $c \vdash^c |t \in \{s_1, s_2\}|_c \leftrightarrow |t = s_1 \vee t = s_2|_c$.

Proof. The direction from left to right is clear from the definitions. For the other direction assume that

$$c \vdash |t = s_1|_c \vee |t = s_2|_c.$$

Suppose that

$$c \vdash |s_1|_c : \tau_1 \quad \text{and} \quad c \vdash |s_2|_c : \tau_2.$$

Hence, in $\mathbf{M_T}$:

$$c \vdash^c |s_1|_c \in V_{\tau_1} \quad \text{and} \quad c \vdash^c |s_2|_c \in V_{\tau_2}.$$

Note that we require the additional assumption of the context c. Hence,

$$c \vdash^c \exists x \in V_{\tau_1} \cdot |t = s_1|_c \wedge |x = s_1|_{c;x:=\tau_1} \vee \exists\, x \in V_{\tau_2} \cdot |t = s_2|_c$$
$$\wedge |x = s_2|_{c;x:=\tau_2}.$$

Hence,

$$c \vdash^c \exists x \in V_{\tau_1} \cdot |x = s_1|_{c;x:=\tau_1} \wedge |x = t|_{c;x:=\tau_1} \vee$$
$$\exists x \in V_{\tau_2} \cdot |x = s_2|_{c;x:=\tau_2} \wedge |x = t|_{c;x:=\tau_2}.$$

Let $V_\tau = V_{\tau_1} \cup V_{\tau_2}$. By lifting

$$c \vdash^c \exists x \in V_\tau \cdot |t = x|_{c:x:=\tau} \wedge (|x = s_1 \vee x = s_2|_c).$$

Lemma 15 (Separation). $\vdash^c |t \in \{x \in s \cdot \phi\}|_c \leftrightarrow |t \in s \wedge \phi[t/x]|_c$.

Proof. By replacement we may assume that $|t|_c, |s|_c$ have the same type relative to c and we concentrate on the case where this is i. The lhs unpacks to

$$succ(t) = |s|_c \wedge |\phi[t/x]|_c.$$

which is exactly the rhs. □

Theorem 4 (Soundness). *Let c cover the sequent $\Gamma \vdash \phi$.*

If $\Gamma \vdash_{\mathbf{M}} \phi$ then $|\Gamma|_c, c \vdash^c |\phi|_c$.

Proof. By induction on the derivations. Given the lemmata we have only to check the structural and the logical rules and the infinity axioms. The former are clear. The logical rules are all easy to verify except for the quantifier rules: we illustrate these with the elimination rule for the case where $c \vdash |s|_c : i$. By induction we obtain

$$\forall x \in I \cdot succ(x) = |s|_c \rightarrow |\phi|_{c;x:=i},$$

$$\exists x \in I \cdot succ(x) = |s|_c \wedge |t = x|_{c;x:=i}.$$

The conclusion now follows by the replacement lemma. The axioms of closure and induction are easy to verify. For the representation axioms we have two parts to verify. Given the definitions, $|0 = \Phi|_c$ is immediate. This leaves to verify the second. We have to show

$$\forall x \in I \cdot |succ(x) = \{x\}|_c.$$

The latter follows immediately by the definition of the translation. □

5.3. Agreement

We now show that stratified wff and terms are, up to equality, preserved by the translation.

Theorem 5. *For each stratified ϕ/s and c which stratifies them we have in* $\mathbf{M_T}$:
(1) $c \vdash^c \phi \leftrightarrow |\phi|_c$,
(2) $c \vdash^c s = |s|_c$.

Proof. By simultaneous induction on the structure of the terms and wff. We begin with the base cases of (1), i.e. equality and membership. We employ a sub-induction on the ranks: it is easy to observe that where the terms are of the same type the new notions of equality and membership are equivalent to the old. For complex wff we illustrate with quantification consider the case where $c \vdash_T |s|_c : P\tau$:

$$|\forall x \in s \cdot \phi|_c = \forall x \in |s|_c \cdot |\phi|_{c;x:=\tau}.$$

By induction, $c \vdash^c s = |s|_c$ and $c; x \in V_\tau \vdash^{c;x:\tau} \phi \leftrightarrow |\phi|_{c;x:=\tau}$. Hence, $c \vdash \forall x \in s \cdot \phi \leftrightarrow |\forall x \in s \cdot \phi|_c$. For terms consider the case where $c \vdash Ps : PP\tau$. By generation, $c \vdash s : P\tau$. By induction, $c \vdash^c s = |s|_c$. Also we know from the nature of $\mathbf{M_T}$ that $c \vdash |s|_c : P\tau$. Hence, by clause (10) of the translation we are done. □

Putting soundness and agreement together we have that $\mathbf{M}$ is a conservative extension of $\mathbf{M_T}$ with respect to stratified sequents.

Theorem 6. *Let $\Gamma \vdash \phi$ be stratified by c*:

If $\Gamma \vdash_{\mathbf{M}} \phi$ then $\Gamma, c \vdash^c \phi$.

Our proofs can be easily modified to provide a proof that **M** is a conservative extension of **KF**.

Theorem 7. (1) *Let c cover* Γ, ϕ. *If* $\Gamma \vdash_{\mathbf{M}} \phi$ *then,* $|\Gamma|_c, c \vdash_{\mathbf{KF}} |\phi|_c$

(2) *For each KF* ϕ *and s and c which covers them,*

$$c \vdash_{\mathbf{KF}} \phi \leftrightarrow |\phi|_c,$$

$$c \vdash_{\mathbf{KF}} s = |s|_c.$$

Proof. Part (1) is obvious given that **M** is a conservative extension of $\mathbf{M_T}$ and that **KF** is an extension of $\mathbf{M_T}$. The proof of (2) proceeds as in the case of **M** but we need to observe that we only employ the apparatus of **KF** since in the separation case we only need **KF**. □

6. Equality rules and completeness

For the type system of the Lambda calculus, $\mathbf{T}A_\lambda$ adding an *equality rule*, which guarantees that the type of a term is preserved by equality, yields *completeness* [2]. We now investigate a similar program for **M**.

6.1. Equality rules

The equality rules take the following shape:

$$eq_1 \frac{c \vdash \phi \ prop \qquad c \vdash_{\mathbf{M}} \phi \leftrightarrow \psi}{c \vdash \psi \ prop}$$

$$eq_2 \frac{c \vdash s_1 : \tau \qquad c \vdash_{\mathbf{M}} s_1 = s_2}{c \vdash s_2 : \tau}$$

The type inference system $\mathbf{T}^e$ is **T** plus eq_1 and eq_2. Observe that the generation lemma now fails. However, we can always postpone the application of these rules to the last stage of the derivation.

Theorem 8 (Postponement).
(1) *If* $c \vdash_{\mathbf{T}^e} \phi \ prop$ *then for some* ψ, $c \vdash_{\mathbf{T}} \psi \ prop$ *and* $c \vdash_{\mathbf{M}} \phi \leftrightarrow \psi$.
(2) *If* $c \vdash_{\mathbf{T}^e} s : \tau$ *then there for some t,* $c \vdash_{\mathbf{T}} t : \tau$ *and* $c \vdash_{\mathbf{M}} s = t$.

Proof. By induction on the derivations. We illustrate (1) where the quantifier rule is the last rule applied:

$$\frac{c, x : \tau \vdash_{\mathbf{T}^e} \phi \ prop \qquad c \vdash_{\mathbf{T}^e} s : P\tau}{c \vdash_{\mathbf{T}^e} \forall x \in s \cdot \phi \ prop}$$

By induction there is a wff ψ and term t such that

$$c,x:\tau \vdash_{\mathbf{T}} \psi\ prop \quad \text{and} \quad c,x \in V_\tau \vdash_{\mathbf{M}} \phi \leftrightarrow \psi,$$

$$c \vdash_{\mathbf{T}} t : P\tau \quad \text{and} \quad c \vdash_{\mathbf{M}} s = t.$$

It follows that

$$c \vdash_{\mathbf{T}} \forall x \in t \cdot \psi\ prop \quad \text{and} \quad c \vdash_{\mathbf{M}} \forall x \in s \cdot \phi \leftrightarrow \forall x \in t \cdot \psi.$$

Now we can apply the eq_1 rule to obtain the conclusion. For (2) we illustrate where the rule for separation is the last rule applied:

$$\frac{c,x:\tau \vdash_{\mathbf{T}^e} \phi\ prop \qquad c \vdash_{\mathbf{T}^e} s : P\tau}{c \vdash_{\mathbf{T}^e} \{x \in s \cdot \phi\} : P\tau}$$

By induction there is a wff ψ and term t such that

$$c,x:\tau \vdash_{\mathbf{T}} \psi\ prop \quad \text{and} \quad c,x \in V_\tau \vdash_{\mathbf{M}} \phi \leftrightarrow \psi,$$

$$c \vdash_{\mathbf{T}} t : P\tau \quad \text{and} \quad c \vdash_{\mathbf{M}} s = t.$$

It follows that

$$c \vdash_{\mathbf{T}} \{x \in t \cdot \psi\} : P\tau \quad \text{and} \quad c \vdash_{\mathbf{M}} \{x \in s \cdot \phi\} = \{x \in t \cdot \psi\}$$

Now we can apply the eq_2 rule to obtain the conclusion. □

6.2. Completeness of $\mathbf{T}^e$

We now show that $\mathbf{T}^e$ is complete in the sense that according to $\mathbf{T}^e$ every expression in $\mathbf{M}$ is stratified. First we require:

Theorem 9. *For each ϕ and s and c which covers them, we have in* $\mathbf{M}$:
(1) $c \vdash \phi \leftrightarrow |\phi|_c$,
(2) $c \vdash s = |s|_c$.

Proof. The main induction is on the structure of the terms and wff. We begin with the base cases of equality and membership. We employ induction on the ranks. We illustrate with equality. We have to show

$$|s_1 = s_2|_c \leftrightarrow s_1 = s_2.$$

We illustrate the equality case where $c \vdash |s_1|_c : i$ and $c \vdash |s_2|_c : P\tau$. By the rank induction hypothesis we obtain

$$c \vdash |s_1 = s_2|_c \leftrightarrow$$

$$\forall x \in I \cdot s_1 = succ(x) \rightarrow x \in s_2 \wedge \forall x \in s_2 \cdot x \in s_1.$$

By numerical induction, $\forall x \in I \cdot s_1 = succ(x) \rightarrow x \in s_2$ is equivalent to $\forall x \in s_1 \cdot x \in s_2$. By extensionality we are finished. □

We can now prove completeness.

Theorem 10 (Completeness). *For each wff/term*:
(1) *If c covers* ϕ *then* $c \vdash_{\mathbf{T}^e} \phi$ *prop*.
(2) *If c covers s then* $c \vdash_{\mathbf{T}^e} s : \tau$ *for some* τ.

Proof. Both follow directly from last theorem. □

Consequently, the addition of such rules make the type system $\mathbf{T}^e$ undecidable.

7. More expressive type theories

Without the *eq* rules much of the set theory lives outside the type system. This parallels the case for the lambda calculus where much of the language is inaccessible if we wish to remain within the confines of the type system $\mathbf{T}A_\lambda$ whose only type constructor is $\Rightarrow$. This has led to the development of richer type systems for the lambda calculus which include Cartesian products, recursive types, polymorphic types, etc. [1]. In this section we begin to explore a similar program.

T imposes the structure of simple type theory upon **M**. A natural extension would move us to the structure imposed by higher order logic. Consequently, we shall illustrate the process of extending the type system by reference to ordered pairs and Cartesian products.

Consider the standard definitions of ordered pairs and Cartesian products given in **M**:

$$(s_1, s_2) \triangleq \{\{s_1\}, \{s_1, s_2\}\},$$

$$s_1 \otimes s_2 \triangleq \{x \in PP(s_1 \cup s_2) \cdot \exists y \in s_1 \cdot \exists z \in s_2 \cdot x = \{\{y\}, \{y, z\}\}\}.$$

From a typed perspective, there would be no point in forming ordered pairs unless they are composed of elements of different types. To achieve this, since ordered pairs employ the pairing construction, we need to be able to construct pairs from sets of different types. However, the type inference rules for pairs does not permit one to assign a type to pairs whose components have different types. A similar problem arises with Cartesian products: under the above representation we require the union of two sets to be well-typed even when the sets are of different types.

7.1. A definitional extension of **M**

To set up the type system we employ a definitional extension of **M** in which the ordered pairs and Cartesian products are added as new primitives. The syntax of terms thus takes the form

$$s ::= x | \Phi | 0 | succ(s) | I\{s, s\} | \cup s | Ps | \{x \in s \cdot \phi\} | (s, s) | s \otimes s$$

We inherit all the rules of **M** for the other constructions. In addition, we require axioms which govern ordered pairs and Cartesian products as new primitives. These are dictated by the content of the above definitions but now taken as *axioms*. This parallels the treatment of the natural numbers

(a) $(s_1,s_2)=\{\{s_1\},\{s_1,s_2\}\}$,

(b) $s_1\otimes s_2=\{x\in PP(s_1\cup s_2)\cdot\exists y\in s_1\cdot\exists z\in s_2\cdot x=\{\{y\},\{y,z\}\}\}$.

Let $\mathbf{M}_\otimes$ be the theory which results from **M** by the addition of these new primitives together with axioms (a) and (b).

Obviously this theory is a definitional extension of **M**. More explicitly, there is an obvious translation $(*)$ of $\mathbf{M}_\otimes$ into **M** which is induced by (a) and (b), i.e.

$$(s_1,s_2)^*=\{\{s_1^*\},\{s_1^*,s_2^*\}\},$$

$$(s_1\otimes s_2)^*=\{x\in PP(s_1^*\cup s_2^*)\cdot\exists y\in s_1^*\cdot\exists z\in s_2^*\cdot x=\{\{y\},\{y,z\}\}\}.$$

The translation neutrally passes through the other expressions so that if ϕ is a wff of **M** then $\phi=\phi^*$.

Theorem 11. *If* $\Gamma\vdash_{\mathbf{M}_\otimes}\phi$ *then* $\Gamma^*\vdash_{\mathbf{M}}\phi^*$.

The difference between two theories, one of which is a definitional extension of the other, is so slight that they are for most purposes treated as one and the same theory. However, the difference is important from the perspective of the type system since otherwise we would not have Unicity.

7.2. The type system $\mathbf{T}_\otimes$

We enrich **T** to cater for ordered pairs and Cartesian products. The types now take the following form:

$$\tau ::= i \mid \tau\otimes\tau \mid P\tau$$

We adopt all the rules of **T** together with the following new rules:

$$\frac{s_1:\tau_1\quad s_2:\tau_2}{(s_1,s_2):\tau_1\otimes\tau_2}\qquad\frac{s_1:P\tau_1\quad s_2:P\tau_2}{s_1\otimes s_2:P(\tau_1\otimes\tau_2)}$$

Call this new system $\mathbf{T}_\otimes$. All the basic results extend from **T** to $\mathbf{T}_\otimes$. In particular, we have the following extensions to the generation lemma.

Lemma 16 (Generation for $\mathbf{T}_\otimes$). (1) *If* $c\vdash(s,t):\sigma$ *then* σ *has the form* $\tau_1\otimes\tau_2$ *and* $c\vdash s:\tau_1$ *and* $c\vdash t:\tau_2$.

(2) *If* $c\vdash s\otimes t:\sigma$ *then* σ *has the form* $P(\tau_1\otimes\tau_2)$ *and* $c\vdash s:P\tau_1$ *and* $c\vdash t:P\tau_2$.

Proof. We extend the induction of Lemma 2 in the obvious way. □

The Unicity lemma, the sub-formula property and the substitution lemma all remain intact when extended to the new theories. All the proofs are routine extensions of the originals.

We next introduce the *universes* determined by these types. Here there are some differences:

$$V_i \triangleq I,$$

$$V_{P\tau} \triangleq PV_\tau,$$

$$V_{\tau_1 \otimes \tau_2} \triangleq V_{\tau_1} \otimes V_{\tau_2}.$$

The structure of our universes is now quite different and so we need to explore matters more carefully. We still have the foundation principle.

Proposition 5. *In* $\mathbf{M}_\otimes$

$$\forall x \in V_\tau \cdot x \notin x.$$

Proof. By induction on the types. We have only to consider the new case, i.e. the induction step for Cartesian products. Suppose that $x \in V_{\tau_1 \otimes \tau_2}$. Then $x = (x_1, x_2)$ for some $x_1 \in V_{\tau_1}$ and $x_2 \in V_{\tau_2}$. Let $y \in x$. Then by the axioms of representation for ordered pairs

$$y = \{x_1\} \vee y = \{x_1, x_2\}.$$

Then suppose that $x \in x$. Then $x = \{x_1\}$ or $x \in \{x_1, x_2\}$. Thus $\{x_1\} \in \{x_1\}$ or $\{x_1, x_2\} \in \{x_1, x_2\}$. In the former case we have $x_1 \in x_1$ but since $x_1 \in V_{\tau_1}$, this contradicts the induction hypothesis. If $\{x_1, x_2\} \in \{x_1, x_2\}$ then $x_1 = \{x_1, x_2\}$ or $x_2 = \{x_1, x_2\}$. Suppose the former. Then again we have: $x_1 \in x_1$. □

The universes are still cumulative.

Proposition 6. *In* $\mathbf{M}_\otimes$, *for each type* τ,

$$V_\tau \subseteq V_{P\tau}.$$

Proof. By induction on the types. The proof is identical to the case of $\mathbf{M}$. □

In the case of $\mathbf{M}$ this resulted in a cumulative linear sequence of universes. This is clearly no longer the case. However, the important property is *inclusion*, i.e. for all types τ_1, τ_2 there exists a type σ such that $V_{\tau_1}, V_{\tau_2} \subseteq V_\sigma$. While this is true in $\mathbf{M}_\otimes$, the proof is more tricky. First observe that we can map the old types to the new ones as follows:

$$i^* = i,$$

$$(P\tau)^* = P(\tau^*),$$

$$(\tau_1 \otimes \tau_2)^* = PP(\max(\tau_1^*, \tau_2^*)).$$

Proposition 7. *In* $\mathbf{M}_\otimes$, *for each type* $V_\tau \subseteq V_{\tau^*}$.

Proof. By induction on the types. For the base case and the power set the verification is trivial. Suppose $z \in V_{\tau_1} \otimes V_{\tau_2}$. Then by induction, $z_1 \in V_{\tau_1} \subseteq V_{\tau_1^*}$ and $z_2 \in V_{\tau_2} \subseteq V_{\tau_1^*}$. Hence, $z = (z_1, z_2) = \{\{z_1\}, \{z_1, z_2\}\} \in V_{PP(\max(\tau_1^*, \tau_2^*))} = V_{(\tau_1 \otimes \tau_2)^*}$. □

Proposition 8 (Inclusion). *In* $\mathbf{M}_\otimes$, *for all types* τ_1, τ_2 *there exists a type* σ *such that type* $V_{\tau_1}, V_{\tau_2} \subseteq V_\sigma$.

Proof. Chose the maximum of $V_{\tau_i^*}$. □

7.3. The stratified theory

The language of the theory $\mathbf{M}_{\mathbf{T}_\otimes}$ is that of $\mathbf{M}_\otimes$. We inherit all the axioms/rules of $\mathbf{M}_\mathbf{T}$ plus the following rules for ordered pairs and Cartesian products:

$$\frac{t_1 \in s_1 \quad t_2 \in s_2}{(t_1, t_2) \in s_1 \otimes s_2} \qquad \frac{t \in s_1 \otimes s_2}{\exists x \in s_1 \cdot \exists y \in s_2 \cdot t = (x, y)}$$

$$\frac{t_1 \in s_1 \quad t_2 \in s_2 \quad t_3 \in s_1 \quad t_4 \in s_2}{(t_1, t_2) = (t_3, t_4) \to t_1 = t_2 \wedge t_3 = t_4}$$

We shall continue to write $\Gamma \vdash^c \phi$ for derivability in this extended theory. One can show, by extending the original proof to these new rules, that:

Theorem 12. *If* $\Gamma \vdash^c \phi$ *then for each* $\gamma \in \Gamma \cup \{\phi\}$ *we have*

$$c \vdash_{\mathbf{T}_\otimes} \gamma \ \textit{prop}$$

7.4. Stratification

Our objective is to prove that any $\mathbf{T}_\otimes$-stratified theorem of $\mathbf{M}_\otimes$ is a theorem of $\mathbf{M}_{\mathbf{T}_\otimes}$. One might expect this result to be forthcoming from the following:

$$\begin{array}{ccc} \mathbf{M}_\otimes & \stackrel{?}{\Rightarrow} & \mathbf{M}_{\mathbf{T}_\otimes} \\ \Downarrow * & & \Downarrow * \\ \mathbf{M} & \stackrel{\|_c}{\Rightarrow} & \mathbf{M}_\mathbf{T} \end{array}$$

Observe that $*$ followed by $\|_c$ yields a translation from $\mathbf{M}_\otimes$ to $\mathbf{M}_\mathbf{T}$ and hence into $\mathbf{M}_{\mathbf{T}_\otimes}$. However, this translation does not preserve the structure of all $\mathbf{T}_\otimes$-stratified expressions but only the $\mathbf{T}$-stratified ones. Indeed the following fails:

$$\textit{If } c \vdash_{\mathbf{T}_\otimes} s : \tau \textit{ then } c^* \vdash_\mathbf{T} s^* : \tau^*$$

In particular, the obvious induction on the derivations fails in the case ordered pairs. From this translation we can only deduce that $\mathbf{M}_{\otimes}$ is a conservative extension of $\mathbf{M}_{\mathbf{T}_{\otimes}}$ for $\mathbf{T}$-stratified expressions whereas we require the result for all $\mathbf{T}_{\otimes}$-stratified expressions. To achieve this we extend the translation $\|_c$ to the whole of $\mathbf{M}_{\otimes}$.

We consider the obvious cases first. Under the old interpretation ordered pairs and were filtered through the pairing construction; now they are directly translated as new primitives.

$$|(s_1,s_2)|_c \triangleq (|s_1|_c,|s_2|_c), \tag{23}$$

$$|s_1 \otimes s_2|_c \triangleq |s_1|_c \otimes |s_2|_c. \tag{24}$$

Everything proceeds as before until we hit the case of pairing. We now interpret

$$|\{s_1,s_2\}|_c \triangleq \{x \in V_\sigma \cdot |x = s_1|_{c;x:=\sigma} \vee |x = s_2|_{c;x:=\sigma}\} \tag{25}$$

where $c \vdash_T |s_i|_c : \tau_i$ and $V_\sigma = V_{\tau_1^*} \cup V_{\tau_2^*}$.

We can now deal with quantification, membership and equality. We have to maintain the representation axioms for ordered pairs and Cartesian products. We thus interpret

$$(|\forall x \in s \cdot \phi|_c \triangleq \forall x \in |\{\{s_1\},\{s_1,s_2\}\}|_c \cdot |\phi[x]|_{c;x:=\mu}$$
$$\text{where } c \vdash |s|_c : \tau_1 \otimes \tau_2 \text{ and } \mu = P(\max(\tau_1,\tau_2)), \tag{26}$$

where $s=(s_1,s_2)$. The interpretation of membership and equality follows suite:

$$|t \in s|_c \triangleq \exists x \in |\{\{s_1\},\{s_1,s_2\}\}|_c \cdot |x = t|_{c;x:=\mu} \tag{27}$$

where $c \vdash |s|_c : \tau_1 \otimes \tau_2$ and $\mu = P(\max(\tau_1,\tau_2))$,

$$|s = t|_c \triangleq \forall x \in |\{\{s_1\},\{s_1,s_2\}\}|_c \cdot |x \in t|_c \wedge |\forall x \in t \cdot x \in s|_c \tag{28}$$

where $c \vdash |s|_c : \tau_1 \otimes \tau_2$.

Now we have to establish that the rhs are stratified. Consider (27). Suppose $c \vdash |t|_c : \tau$. We take the rank of a translated equality/membership wff to be given via the rank of the translated types under $*$. Thus the rank of $|x=t|_{c;x:=\mu}$ is $\mu^* + \tau^*$ whereas the rank of $|t \in s|_c$ is $\mu^* + 1 + \tau^*$.

Finally we need to deal with the cases of the set terms. The following unpack to yield the explicit translations:

$$|Ps|_c \triangleq P|\{\{s_1\},\{s_1,s_2\}\}|_c \quad \text{when } c \vdash |s_1|_c : \tau_1 \otimes \tau_2, \tag{29}$$

$$|\cup s|_c \triangleq \cup|\{\{s_1\},\{s_1,s_2\}\}|_c \quad \text{when } c \vdash |s_1|_c : \tau_1 \otimes \tau_2, \tag{30}$$

$$|\{x \in s \cdot \phi\}|_c \triangleq \{x \in |\{\{s_1\},\{s_1,s_2\}\}|_c \cdot |\phi|_{c;x:=\mu}\}, \tag{31}$$

$$\text{where } c \vdash |s|_c : \tau_1 \otimes \tau_2 \text{ and } \mu = P(\max(\tau_1,\tau_2)). \tag{32}$$

By extending the original inductions to the new cases we can show that

Theorem 13. (1) *For each e and covering c,*

$|e|_c$ *is* $\mathbf{T}_\otimes$*-stratified by c*

(2) *Let c cover the sequent* $\Gamma \vdash \phi$.

If $\Gamma \vdash_{\mathbf{M}_\otimes} \phi$ *then* $|\Gamma|_c,\ c \vdash^c |\phi|_c$.

(3) *For each* ϕ, *s and c which* $\mathbf{T}_\otimes$*-stratifies them we have*:

(a) $c \vdash^c \phi \leftrightarrow |\phi|_c$,

(b) $c \vdash^c s = |s|_c$.

(4) *Let* $\Gamma \vdash \phi$ *be a sequent of* $\mathbf{M}_\otimes$ *which is* $\mathbf{T}_\otimes$ *stratified by c.*

If $\Gamma \vdash_{\mathbf{M}_\otimes} \phi$ *then* $\Gamma,\ c \vdash^c \phi$.

Completeness also goes through in the obvious way: we need to add the equality rules as before. Thus the whole theory extends to the enriched type system.

There are undoubtedly many other kinds of extension worthy of consideration such as the schema types of Z but this extension is routine given the Cartesian product case. In any case, we have done enough to illustrate the central issues which arise. The important moral to draw from such extensions is that this approach to typed set theory enables one to have the expressive power of set theory and that one can maintain the standard representation of these notions, while preserving an appropriate type regime. More adventurous type systems which involve dependent types and the generalized type systems of combinatory logic [1] might be explored.

References

[1] H.P. Barendregt, Lambda calculus with types, in: S. Abramsky, D.M. Gabbay, T.S.E. Maibaum (Eds.), Handbook of Logic in Computer Science, Oxford Science Publications, 1992, pp. 118–310.
[2] H.P. Barendregt, C. Coppi, A filter lambda model and the completeness of type assignment, J. Symb. Logic 48 (4) (1983) 931–940.
[3] S. Brien, A logic and model for the Z-standard, D. Phil. Thesis, Oxford University, 1999.
[4] A.Z. Diller, An Introduction to Formal Methods, Wiley, New York, 1990.
[5] R. Goldblatt, Topoi, North-Holland Studies in Logic Vol. 98 (1984).
[6] J. Fitzgerald, P.G. Larsen, Modelling Systems, Cambridge University Press, Cambridge, 1998.
[7] G. Forster, Weak systems of set theory related to HOL, in: Th.F. Melham, J. Camilleri (Eds.), Higher Order Logic Theorem Proving and its Applications: Proc. 7th International Workshop, Valletta, Malta, September 1994, Lecture Notes in Computer Science, Vol. 859, Springer, Berlin, 1994.
[8] C.B. Jones, Systematic Software Development using VDM, Prentice-Hall Series in Computer Science, London, 1986.
[9] A.R.D. Mathias, The strength of Maclane set theory Ann. Pure Appl. Logic, to appear.
[10] R. Milnor, A theory of type polymorphism in programming, J. Comput. System Sci. 17 (1978) 348–375.
[11] J.E. Nicholls, (Ed.), Z-Notation, version 1.2, 1995.
[12] J.E. Nicholls, (Ed.), Z-Notation, version 1.3, 1998.
[13] J.M. Spivey, Understanding Z, Cambridge Tracts in Theoretical Computer Science, 3. Cambridge, 1988.
[14] R. Turner, Sets, types and type-checking, J. Logic Comput. 9 (1999) 959–975.
[15] J. Woodcock, J. Davies, Using Z-specifications, Refinement and Proof, Prentice-Hall, Englewood Cliffs, NJ, 1996.